
**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH**

**JAMIE KILGORE and B.E., individuals on
behalf of themselves and all others similarly
situated,**

Plaintiffs,

vs.

**EASTERSEALS-GOODWILL NORTHERN ROCKY
MOUNTAIN, INC., a Montana Corporation,**

Defendants.

MEMORANDUM DECISION AND ORDER

Case No. 2:22CV728 DAK-CMR

Judge Dale A. Kimball

This matter is before the court on Defendant Easterseal-Goodwill Northern Rocky Mountain, Inc.'s ("Defendant") Motion to Dismiss. On May 18, 2023, the court held a hearing on the motion via Zoom videoconferencing. At the hearing, Raina C. Borrelli and Jason R. Hull represented Plaintiffs Jamie Kilgore and B.E. ("Plaintiffs"), and Douglas C. Smith represented Defendant. At the conclusion of the hearing, the court took the motion under advisement. The court has carefully considered the memoranda filed by the parties, the arguments made by counsel at the hearing, and the law and facts pertaining to the motions. Now being fully advised, the court issues the following Memorandum Decision and Order denying without prejudice Defendant's Motion to Dismiss and permitting a 3-month discovery period for Plaintiffs to conduct discovery related to Article III standing.

BACKGROUND

This case is a proposed class action pertaining to a data breach of Plaintiffs' work email accounts in 2021. Plaintiffs worked for a job skill training non-profit company, Defendant

Easter-Seals-Goodwill, which had retail store locations in Idaho, Montana, Utah, and Wyoming. They claim that their emails contained sensitive and confidential employee and client information. They further allege that when Defendant finally announced the Data Breach, it deliberately underplayed the severity of the breach and misrepresented that “we are not aware of any reports of improper use of information as a direct result of this incident,” even though Defendants knew cybercriminals had infiltrated its systems.

Plaintiffs contend that Defendant’s failure to timely detect and report the Data Breach made victims vulnerable to identify theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their personal identifiable information (“PII”). Thus, Plaintiffs and members of the proposed nationwide Class claim that they are victims of Defendant’s negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class allege that they trusted Defendant with their PII but that Defendant betrayed that trust because it failed to properly use up-to-date security practices to prevent the Data Breach.

Ms. Kilgore’s Claimed Injuries

Since the Data Breach, Ms. Kilgore alleges the following injuries resulting from the Data Breach:

- she has experienced fraudulent attempts to use her PayPal account to purchase firearms;
- she has received spam texts and phone calls;
- she has spent, and will have to spend, considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft;

- her personal financial security has been jeopardized and there is uncertainty over what personal information was revealed in the Data Breach;
- she has suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property;
- her privacy has been invaded by the access to and exfiltration of her PII, which is now in the hands of third-parties not authorized to view or possess her PII;
- she has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of criminals; and
- she has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy, fraud that he suffered, and risk of future harm.

B.E.'s Claimed Injuries

Since the Data Breach, B.E. alleges the following injuries resulting from the Data Breach:

- he has experienced fraudulent attempts to use his Visa card and Costco membership to purchase products;
- he has spoken with all three major credit bureaus and frozen his credit. He has paid money to each of the bureaus for fraud protection services and continues to incur monthly expenses to try to protect his identity;
- he has received phishing emails since the Data Breach;
- he has spent, and will have to spend, considerable time and effort over the coming years monitoring his accounts to protect himself from identity theft. Plaintiff's personal financial security has been jeopardized and there is uncertainty over what personal information was revealed in the Data Breach;
- he has suffered actual injury in the form of damages to and diminution in the value of his PII;
- his privacy has been invaded by the access to and exfiltration of his PII, which is now in the hands of third parties not authorized to view or possess his PII;

- he has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals; and
- he has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy, fraud that he suffered, and risk of future harm.

Claimed General Injuries Suffered by Plaintiffs and Proposed Class Members

- According to experts, one out of four data breach notification recipients become a victim of identity fraud;
- monetary losses and lost time; and
- they have also suffered or are at an increased risk of suffering:
 - a. the loss of the opportunity to control how their PII is used;
 - b. the diminution in value of their PII;
 - c. the compromise and continuing publication of their PII;
 - d. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
 - e. lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
 - f. delay in receipt of tax refund monies;
 - g. unauthorized use of stolen PII; and
 - h. the continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession

Plaintiffs have asserted causes of action for negligence; negligence per se; breach of contract, including breach of the implied covenant of good faith and fair dealing; unjust

enrichment; invasion of privacy; and requests for declaratory judgment and injunctive relief. Through the instant motion, Defendant has moved to dismiss the Complaint under FRCP 12(b)(1) for lack of Article III standing and under FRCP 12(b)(6) for failure to state a claim.

DISCUSSION REGARDING ARTICLE III STANDING

To demonstrate standing, a plaintiff must show that she has suffered an “injury in fact” that is “fairly traceable” to the defendant’s actions and that is “likely to be redressed” by the relief she seeks. *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547, (2016) (quoting *Lujan v. Defs. of Wildlife, Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal quotations and citations omitted)).

A Rule 12(b)(1) challenge to subject matter jurisdiction can be either facial or factual. *See Ratheal v. United States*, No. 20-4099, 2021 WL 3619902, at *3 (10th Cir. Aug. 16, 2021). A facial attack “questions the sufficiency of the complaint,” and when “reviewing a facial attack on the complaint, a district court must accept the allegations in the complaint as true.” *Id.* A factual attack goes beyond allegations in the complaint and challenges the facts on which subject matter jurisdiction depends. *Id.* When reviewing a factual attack, a court “may not presume the truthfulness of the complaint’s factual allegations,” and may consider affidavits and other documents to resolve disputed jurisdictional facts under Rule 12(b)(1) without converting the motion to a summary judgment motion. *Id.*

In support of the instant Motion to Dismiss, Defendant provided a Declaration from John Martin, its Chief Legal and Privacy Officer. In the Declaration, Mr. Martin challenges the veracity of the Complaint’s allegations that pertain to Plaintiffs’ standing. He states that there is no indication that the cyberattackers targeted “personal information of private persons during

the data security incident.” To the contrary, he states, the terms used by the threat actors to search the accessed Defendant’s systems strongly indicate their motive was to obtain information to attempt to trick Defendant to redirect wire transfers or direct deposits to accounts controlled by the attackers.

Defendant was able to identify search terms used by the unauthorized persons who accessed employee email accounts. Search terms used included the terms “account payable,” “invoice,” “direct deposit” and “ach.” He claims that if the purpose of the unauthorized access was to obtain personal information about employees or others, it would be expected to see that the attackers used search terms such as “social security number,” “SSN,” “date of birth,” “DOB”, “driver’s license” or “DL” to find that kind of information in the email accounts. Mr. Martin also asserts that the unauthorized persons who accessed the email accounts did not use any of these search terms and that the search terms used suggest the purpose of the attack was not to obtain personal identifying information regarding employees.

Defendants argue that courts routinely dismiss cases like this where there is no indication “of a motive to steal the PII for identity theft or fraud.” *Quintero v. Metro Santurce, Inc.*, 2021 WL 5855752 (D.P.R. Dec. 9, 2021); *see also Travis v. Assured Imaging LLC*, 2021 WL 1862446, at *17 (D. Ariz. May 10, 2021) (dismissing data security action for lack of standing, partly because allegations did not indicate that data was taken in a “manner that suggests it will be misused.”). Defendants argue that Plaintiffs have not and cannot meet their burden to offer evidence demonstrating standing through “certainly impending” risk of future harm. *Clapper v. Amnesty Int’l*, 568 U.S. 398, 408 (2013).

Moreover, Defendant claims that all the alleged injuries do not withstand this factual challenge because the claimed harm has no nexus with the Data Breach. *See Spokeo*, 136 S.Ct. at 1547. Specifically, the potentially accessed information in the affected email accounts did not include Ms. Kilgore's PayPal information or her phone number. Regarding B.E., Defendant argues that the potentially accessed information in the email accounts did not include an email address for the employee of Defendant who works in Utah and has the initials B.E. Defendant contends, and the court agrees, that Plaintiffs have not offered evidence to meet their burden to demonstrate a concrete injury traceable to this cyberattack on Defendant.

Given Defendant's factual attack on standing, the court finds that Plaintiffs have thus far failed to satisfy their burden to demonstrate an injury-in-fact that is fairly traceable to the Data Breach for purposes of Article III standing. Despite Defendant's arguments and the Declaration or Mr. Martin, Plaintiffs did not file a motion for leave to conduct discovery to oppose Defendant's factual attack. They did, however, note in their opposition memorandum that the court "should not grant Defendant's motion based on [the allegations in the Declaration]. Instead, it should order discovery on the matter so that Plaintiff may scrutinize them." ECF No. 16 at 5. Therefore, out of an abundance of caution, the court will permit a three-month discovery period—ending on October 20, 2023—for Plaintiffs to conduct limited discovery related to establishing Article III standing, without which, this court lacks jurisdiction.¹

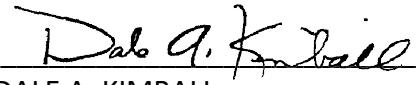
Accordingly, for the foregoing reasons, Defendant's Motion to Dismiss [ECF No. 13] is DENIED without prejudice to renew the motion after Plaintiffs have conducted discovery

¹ Because it is not clear that this court has jurisdiction over this matter, the court declines to rule on Defendant's arguments under Rule 12(b)(6) that Plaintiffs have failed to state a claim for relief.

related to Article III standing. The discovery period ends on October 20, 2023, unless a motion for an extension of time, setting forth good cause, is filed and granted before that date.

DATED this 18th day of July, 2023.

BY THE COURT:



DALE A. KIMBALL
United States District Judge